	Application No.	Applicant(s)
Notice of Allowability	09/552,115	KIPNIS ET AL.
	Examiner	Art Unit
	Shin-Hon Chen	2131
The MAILING DATE of this communication ap All claims being allowable, PROSECUTION ON THE MERITS herewith (or previously mailed), a Notice of Allowance (PTOL-8 NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT of the Office or upon petition by the applicant. See 37 CFR 1.3	S (OR REMAINS) CLOSED 5) or other appropriate comm RIGHTS. This application is	in this application. If not included nunication will be mailed in due course. THIS
1. This communication is responsive to <u>Amendment filed on</u>	<u>n 11/29/05</u> .	
2. A The allowed claim(s) is/are 1-5, 7-14, 18-22, 24-31, and	<u>35-44</u> .	
<ul> <li>3.  Acknowledgment is made of a claim for foreign priority</li> <li>a)  All b)  Some* c)  None of the:</li> <li>1.  Certified copies of the priority documents had</li> <li>2.  Certified copies of the priority documents had</li> </ul>	ve been received.	
Copies of the certified copies of the priority of International Bureau (PCT Rule 17.2(a)).      Certified copies not received:	• •	
Applicant has THREE MONTHS FROM THE "MAILING DATE noted below. Failure to timely comply will result in ABANDON THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.		e a reply complying with the requirements
4. A SUBSTITUTE OATH OR DECLARATION must be sub INFORMAL PATENT APPLICATION (PTO-152) which g		
<ol> <li>CORRECTED DRAWINGS (as "replacement sheets") m</li> <li>(a) ☐ including changes required by the Notice of Draftspe</li> <li>1) ☐ hereto or 2) ☐ to Paper No./Mail Date</li> <li>(b) ☐ including changes required by the attached Examine Paper No./Mail Date</li> </ol>	erson's Patent Drawing Revie 	,
Identifying indicia such as the application number (see 37 CFR each sheet. Replacement sheet(s) should be labeled as such in		
DEPOSIT OF and/or INFORMATION about the department attached Examiner's comment regarding REQUIREMEN		
Attachment(s)		
<ol> <li>Notice of References Cited (PTO-892)</li> <li>Notice of Draftperson's Patent Drawing Review (PTO-948)</li> </ol>		nformal Patent Application (PTO-152)
,	Paper No	Summary (PTO-413), ./Mail Date
<ul> <li>3.  Information Disclosure Statements (PTO-1449 or PTO/SE Paper No./Mail Date 9/5/00</li> <li>4.  Examiner's Comment Regarding Requirement for Deposit of Biological Material</li> </ul>		s Amendment/Comment s Statement of Reasons for Allowance
	9. 🗌 Other	- n 01
		Hmshu
		AYAZ SHEIKH
		SUPERVISORY PATENT EXAMINER TECHNOLOGY CENTER 2100

Application/Control Number: 09/552,115 Page 2

Art Unit: 2131

## **DETAILED ACTION**

1. Claims 1-5, 7-14, 18-22, 24-31, and 35-44 are allowed. Claims are renumbered as 1-36.

## Allowable Subject Matter

The following is an examiner's statement of reasons for allowance: The closes prior art of record discloses a digital signature method that solves a set of equations as a whole by hiding in the polynomial equations a specific mathematical structure derived from a different mathematical field. The prior art of record individually or in combination does not explicitly disclose the set of equations S1 has two types of variables: x variable and y variables. The set of equations S1 is obtained from a set of equations S2 having another set of variables a1,..., an+v that replaces the set x1,...,xn+v in S1; the variables a1,...,an+v can be divided into two groups: the first group includes n variables which are the "oil" variables, and the second group includes the remaining v variables which are the "vinegar variables" and the number of v of "vinegar" variables are greater than the number n of "oil" variables in light of other features disclosed in independent claims.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

## Response to Arguments

3. Applicant's arguments, see Remarks, filed 11/29/05, with respect to claims 1-5, 7-14, 18-22, 24-31, and 35-42 have been fully considered and are persuasive. The rejection of claims 1-5, 7-14, 18-22, 24-31, and 35-42 has been withdrawn.

Application/Control Number: 09/552,115 Page 3

Art Unit: 2131

allowance.

4. The applicant has amended claims to overcome the 101 rejection as set forth in previous office action. Therefore, claims 1-5, 7-14, 18-22, 24-31, and 35-44 are in condition for

## Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen Examiner

Art Unit 2131

SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

SC